CLAIMS

For the convenience of the Examiner, all claims have been presented whether or not an amendment has been made. The claims have been amended as follows:

1. **(Currently Amended)** A method of detecting a class of viral code, comprising:

heuristically analyzing a subject file **to detect at least one class of viral code, the heuristic analysis based at least in part on one or more rules;**

identifying at least one new characteristic of a viral code;

generating at least one new rule, the at least one new rule based at least in part on the at least one new characteristic;

generating ~~to generate~~ a set of flags **based at least in part on the heuristic analysis** ~~along with statistical information~~;

using the set of flags ~~with statistical information~~ to perform at least one search for a scan string and/or a statement type in the subject file; and

triggering a positive detection alarm if each of the at least one search is found at least a corresponding predetermined number of times.

2. **(Original)** The method of Claim 1, wherein the subject file includes source code in a predetermined programming language.

3. **(Original)** The method of Claim 2, wherein the predetermined programming language is a script language.

4. **(Original)** The method of Claim 1, wherein the subject file includes a file for a predetermined word processor.

5. **(Currently Amended)** The method of Claim 1, wherein at least one flag in the set of flags corresponds to a copy operation associated with **a viral code** ~~one~~ of the **at least one** class of viral code.

6. **(Original)** The method of Claim 1, wherein at least one flag in the set of flags corresponds to an operation for adding data from a string to a target module.

7. **(Original)** The method of Claim 1, wherein at least one flag in the set of flags corresponds to an operation for importing another code.

8. **(Original)** The method of Claim 1, wherein at least one flag in the set of flags corresponds to an operation for disabling virus protection features in a target application.

9. **(Original)** The method of Claim 1, wherein the searched statement type corresponds to an operation for disabling functionalities in a target application.

10. **(Previously Presented)** The method of Claim 1, wherein the searched statement type corresponds to an operation for overwriting system macros.

11. **(Currently Amended)** A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for detecting a class of viral code, the method steps comprising:

heuristically analyzing a subject file **to detect at least one class of viral code, the heuristic analysis based at least in part on one or more rules;**

identifying at least one new characteristic of a viral code;

generating at least one new rule, the at least one new rule based at least in part on the at least one new characteristic;

generating ~~to generate~~ a set of flags **based at least in part on the heuristic analysis** ~~along with statistical information~~;

using the set of flags ~~with statistical information~~ to perform at least one search for a scan string and/or a statement type in the subject file; and

triggering a positive detection alarm if each of the at least one search is found at least a corresponding predetermined number of times.

12. **(Currently Amended)** A computer system, comprising:

a processor; and

a program storage device readable by the computer system, tangibly embodying a program of instructions executable by the processor to perform method steps for detecting a class of viral code, the method steps comprising:

heuristically analyzing a subject file **to detect at least one class of viral code, the heuristic analysis based at least in part on one or more rules;**

identifying at least one new characteristic of a viral code;

generating at least one new rule, the at least one new rule based at least in part on the at least one new characteristic;

~~to generate~~ generating a set of flags **based at least in part on the heuristic analysis** ~~along with statistical information~~;

using the set of flags ~~with statistical information~~ to perform at least one search for a scan string and/or a statement type in the subject file; and

triggering a positive detection alarm if each of the at least one search is found at least a corresponding predetermined number of times.

13. **(Currently Amended)** A computer data signal embodied in a transmission medium which embodies instructions executable by a computer for detecting a class of viral code, comprising:

a first segment including heuristic analyzer code to**:**

heuristically analyze a subject file to **detect at least one class of viral code, the heuristic analysis based at least in part on one or more rules;**

identify at least one new characteristic of a viral code;

generate at least one new rule, the at least one new rule based at least in part on the at least one new characteristic;

generate a set of flags **based at least in part on the heuristic analysis** ~~along with statistical information~~;

and

a second segment including scanner code using the set of flags ~~with statistical information~~ to perform at least one search for a scan string and/or a statement type in the subject file, and triggering a positive detection alarm if each of the at least one search is found at least a corresponding predetermined number of times.

14. **(Currently Amended)** An apparatus for detecting a class of viral code, comprising:

an heuristic analyzer~~, wherein the heuristic analyzer analyzes~~ **comprising:**

an heuristic engine operable to:

heuristically analyze a subject file to **detect at least one class of viral code, the heuristic analysis based at least in part on one or more rules;**

identify at least one new characteristic of a viral code; and

generate a set of flags **based at least in part on the heuristic analysis** ~~along with statistical information~~;

and

a learning module operable to generate at least one new rule, the at least one new rule based at least in part on the at least one new characteristic;

and

a search component, wherein the search component uses the set of flags ~~with statistical information~~ generated by the heuristic analyzer to perform at least one search for a scan string and/or a statement type in the subject file, and triggers a positive detection alarm if each of the at least one search is found at least a corresponding predetermined number of times.

15. **(Currently Amended)** The apparatus of Claim 14, wherein the heuristic analyzer **further comprises a memory module operable to store the one or more rules.** ~~is rule-based and comprises a heuristic engine and heuristic rules.~~

16. **(Currently Amended)** The apparatus of Claim 15, wherein the ~~heuristics~~ **heuristic** engine **is further operable to** ~~, using heuristic rules, parses~~ **parse** the subject file **using the one or more rules**.

17. **(Currently Amended)** The apparatus of Claim 15, wherein the ~~heuristics~~ **one or more** rules include sets of heuristic flags stored in a rules table.

18. **(Original)** The apparatus of Claim 14, wherein the search component is rule-based and comprises a search engine and viral code class rules.

19. **(Original)** The apparatus of Claim 14, wherein the search component is a neural network.

20. **(New)** The method of Claim 1, wherein the at least one search is performed using a neural network.